Guest Editorial Preface

Special Issue on "Decision Making in Cybersecurity"

Brian Nussbaum, College of Emergency Preparedness, Homeland Security, and Cybersecurity (CEHC), University at Albany, USA

Unal Tatar, College of Emergency Preparedness, Homeland Security, and Cybersecurity (CEHC), University at Albany, USA

Cybersecurity has grown from a small piece of information technology to a major component of modern corporate risk, national foreign policy, social well-being, and increasingly – with the proliferation of cyber-physical systems – a major component of modern health and safety efforts. If - as the engineer, entrepreneur, and venture capitalist Marc Andreessen said in 2011 that "software is eating the world," that is software increasingly manages and oversees functions previously done with mechanical and organizational systems - then securing that software (and the hardware that run that software) is becoming ever more important for the safe, secure, and efficient operation of the modern world.

Cybersecurity discussions have long focused on data breaches at large retailers, the theft and misuse of financial or credit card data, and the inability to protect personally identifiable information. More recently, ransomware attacks and large-scale organizational doxing or email dumps have shown the profound impact that cyber attacks can have on organizations of all types. High-profile cyber-attacks on water infrastructure, hospitals, electrical power systems, and communications systems have shown the ways in which cybersecurity has become a key operational risk for modern infrastructure. When combined with the growth (or at least growth in well-documented cases) of nation-state espionage and cyber conflict among geopolitical rivals and adversaries, the cyber risk landscape seems to be growing rapidly

The papers in this special issue cover a number of key issues in the space of cybersecurity decision-making. This includes models for assessing and understanding cyber risks and challenges, how to quantify and measure various characteristics of cybersecurity, thinking systematically about serious cyber risks and conflicts, and how cyber practitioners and professionals address those tasks confront them.

Three papers here focus on the application of new or different lenses to thinking about cyber risk.

In "Complex System Governance as a Foundation for Enhancing Cybersecurity of Cyber-Physical Systems," Polinpapilinho F Katina and Omer Keskin adopt and adapt the literature of complex system governance into cybersecurity decision making in the particular context of cyber-physical systems.

In "COVID-19 and Biocybersecurity's Increasing Role on Defending Forward," Xavier Palmer, Lucas Potter, and Saltuk Karahan propose a new conception that combines cybersecurity and biosecurity into "biocybersecurity" as a way of thinking about the increasing overlap between security issues with both information technology and biotechnology.

In "Commissioning Development to Externals: Addressing Infosec Risks Upfront," Yasir Gocke addresses one of the hottest topics in cybersecurity, supply chain risks. Using legal analysis and

assessing organizational strategies and mitigations, this paper examines the challenges posed by allowing vendors, contractors, and external providers to essential business services and the related information security risks.

Two more papers focus on measurement and quantification issues in cybersecurity.

In "Enhancing Cyberweapons Effectiveness Methodology With SE Modeling Techniques: Both for Offense and Defense," Pinto, Zurasky, Elakramine, El Amrani, Jaradat, Kerr, and Dayarathna both adopts another conceptual framework (systems engineering) but applies that approach to measuring and assessing the effectiveness of cyber weapons and attack methodologies.

In "A Monte-Carlo Analysis of Monetary Impact of Mega Data Breaches," Canan, Poyraz, and Akil apply mathematical techniques to improve the understanding of the financial consequences of large-scale data breaches, a key to improving the understanding of the societal impacts of cyber incidents.

Each of these papers brings innovative approaches to understanding how cybersecurity decisions are made and how decision-makers can be supported for well-informed decisions. Innovating in key areas of cyber decision making – from measurement to assessment to mitigation choices – is the only way in which the ever-growing problem of cyber risk can be made more tractable.

Brian Nussbaum
Unal Tatar
Guest Editors
IJCWT